ARCTIC WOLF

THE LEADER IN SECURITY OPERATIONS

# Proposal Overview for:

Edina Public Schools

DEFINING EXCELLENCE

## END CYBER RISK

# Proposal Contents

# Executive Summary

## Arctic Wolf Security Operations-as-a-Service

### Current State Challenges

The cybersecurity industry has an effectiveness problem. Every year new technologies, vendors, and solutions emerge, and yet despite this constant innovation we continue to see high profile breaches in the headlines. All organizations know they need better security, but the dizzying array of options leaves resource-constrained IT and security leaders wondering how to proceed. Arctic Wolf's point of view is that organizations need to do three core things to finally get the security effectiveness they've been looking for:

### Keys to Closing the Gap

**01**

Optimize your existing IT and security controls for better prevention, and then send all telemetry to a cloud platform for storage, enrichment, and analysis.

**02**

Add external expertise to establish 24x7 monitoring, threat hunting, and triage so that you can quickly identify and respond to advanced threats, critical vulnerabilities, and lurking misconfigurations.

**03**

Continually review your cybersecurity posture and work with experts who know your environment well enough to recommend strategic actions that will make it stronger.

Taking these three steps will deliver the security effectiveness that organizations are seeking. Key to this effectiveness is the injection of human expertise into the process. One of the reasons cybersecurity is so hard is because the attackers are smart, capable humans who can adapt to technology enhancements implemented by defenders. As a result, the winning strategy for defenders must also include a human element. Finding the right way to add this human element, however, has been a major challenge for the industry.

# Executive Summary

## Strategic Initiative: *Enhance Security and Visibility*

### Challenge

- ISD 273's in-house security team is extremely constrained and is not able to monitor their environment, all while keeping security related projects moving forward to improve on the organization's security posture.
- Today ISD 273 has Splunk implemented as a SIEM but it's not capturing all logs and is burdensome to maintain and tune. Most importantly, Adam is the only person with any expertise making the ability to monitor and detect threats 24x7x365 impossible.
- ISD 273 utilizes multiple security tools and would benefit from strategic services to identify overlap and opportunities to improve on security posture.
- **Key Drivers:** Holistic Visibility, Faster Intrusion Detection, Team Enhancement, Compliance Attestation

### Desired Outcome

- Full-functioning cloud-integrated SOC service that can leverage existing security tools to provide visibility, monitoring, response and remediation of all security events and incidents.
- True 24X7X365 eyes on glass coverage with containment ability throughout the night.
- Improve mean time to detection and implement faster incident response. Partnership should be able to contain network flow and/or devices for the customer.
- Deliver additional compliance efficiencies and provide reporting to back compliance attestation.
- Streamline operations so that the overall risk profile is better managed and reduced.
- Create a partnership that will raise security profile and fill as many gaps as possible – strategic guidance, planning, benchmarking, and up to date threat awareness.

### Proposed Solution

- Replace Splunk and stand-up Arctic Wolf which provides a fully managed SIEM and service focused on detection and incident response.
- **Implement Arctic Wolf Managed Detection and Response**
  - 24X7X365 Coverage
  - Fully managed & hosted SIEM
  - Gain broad visibility across endpoints, network and cloud – **Unlimited** log ingestion
  - Vendor neutral provider that does not force **lock-in** behavior allowing customers to choose the best-of bread security tools.
  - **Unlimited** Access to security professionals complimented by named resources and a personalized white glove service.

# What we've heard from your team

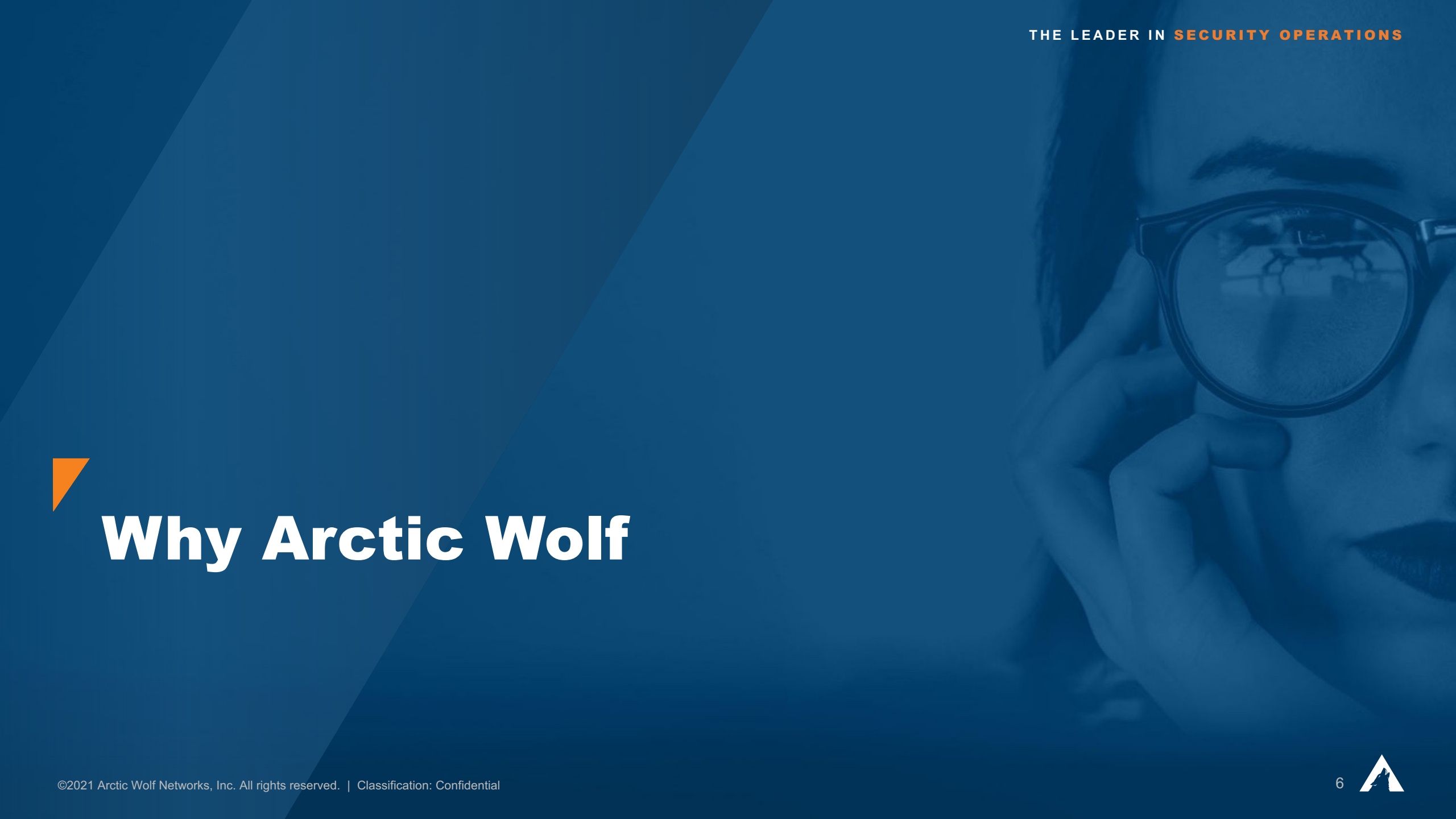


## Current Challenges

1. ISD 273 has a very lean IT team yet a wide array of responsibilities to support the entire school Currently, Adam is the only person with any expertise managing Splunk and therefore doesn't have the bandwidth to operationalize it 24x7x365 on top of his other duties. It is not realistic for ISD 273 to build out their own SOC as it would take multiple hires and hundreds of thousands of dollars invested into additional security tools.
2. ISD 273 has existing identity, cloud, endpoint, and network security tools in place today and desires additional seasoned security professionals to augment team with threat triage, correlation, analysis, strategic guidance, unlimited customized tuning with environmental hardening and continuous security improvement.
3. Interest in human-led, proactive threat hunting over basic "alert-response" and typical operational-level managed services.

## Negative Impact on Business Initiative

1. Massive risk to the district's reputation which would ultimately result in a loss to enrollment from Cyber attack and/or inability to prevent, detect, respond and remediate quickly.
2. Reactive response to current security concerns is a distraction to already burdened staff and existing security initiatives and projects.
3. Inability to identify dormant vulnerabilities and threats in existing environment across all attack surfaces creates a larger risk with potential negative system impact.



# Why Arctic Wolf

# Arctic Wolf Overview

Arctic Wolf® is the market leader in security operations. Using the cloud-native Arctic Wolf® Platform, we provide security operations as a concierge service. Highly trained Concierge Security® experts work as an extension of your team to provide 24x7 monitoring, detection, and response, as well as ongoing risk management to proactively protect systems and data while continually strengthening your security posture.

The cybersecurity industry has an **effectiveness** problem.

| 3,000 | $120B | 3,950 |
|---|---|---|
| Vendors | Total Spend | Reported Breaches |

## About Arctic Wolf

| 2012 | 1,900+ | 3,500+ |
|---|---|---|
| Founded | Employees | Customers |

Gartner COOL VENDOR

500 Technology Fast 500 2019 NORTH AMERICA Deloitte.

2018 WINNER

RED HERRING 100 WINNER N. AMERICA

SC awards Winner

GDPR READY

SOC 2 TYPE 2

Privacy Shield Compliant

CERTIFIED ISO 27001 CERTIFIED

## Industry Cybersecurity Challenges

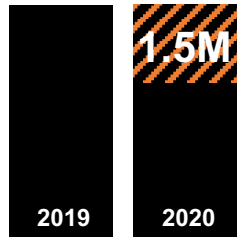
**314 DAYS**

| 230 Days | 84 Days |
|---|---|
| Mean Time to Identify (MTTI) | Mean Time to Contain (MTTC) |

*Source: 2019 Ponemon Cost of Data Breach Incident Report*


of organizations are unable to process +60% of their security data

*Source: Gartner*




The security skills gap through 2020

*Source: Gartner*

## Audit/Compliance Drivers

**PCI DSS** **FFIEC-NCUA** **HIPAA** **NIST 800-171** **23 NYCRR 500**

## Better Protection Against All Attack Types

**Dwell Time**
**0:30**
Industry average time to identify an intrusion is 206 days. Arctic Wolf does it in 30 minutes or less.

**Phishing**
**18%**
Of customers have phishing activity that is missed by email security but caught by Arctic Wolf

**Advanced Threats**
**43%**
Of customers have advanced threat activity being missed by security tools but caught by Arctic Wolf

**Account Takeover**
**70%**
Of customers have some PII exposure and 5.5% have plaintext passwords exposed online

**Unpatched Vulnerabilities**
**35%**
Reduction in time to patch critical vulnerabilities after activating Arctic Wolf

## Arctic Wolf Helps Detect and Respond to the Top 5 Attack Vectors:

- Malware/Ransomware
- Phishing
- PUP Adware
- Account Hijacking
- Unpatched Outdated Software


**Four North American SOCs**

**Eden Prairie, MN | San Antonio, TX**
**Provo, UT | Waterloo, ON**

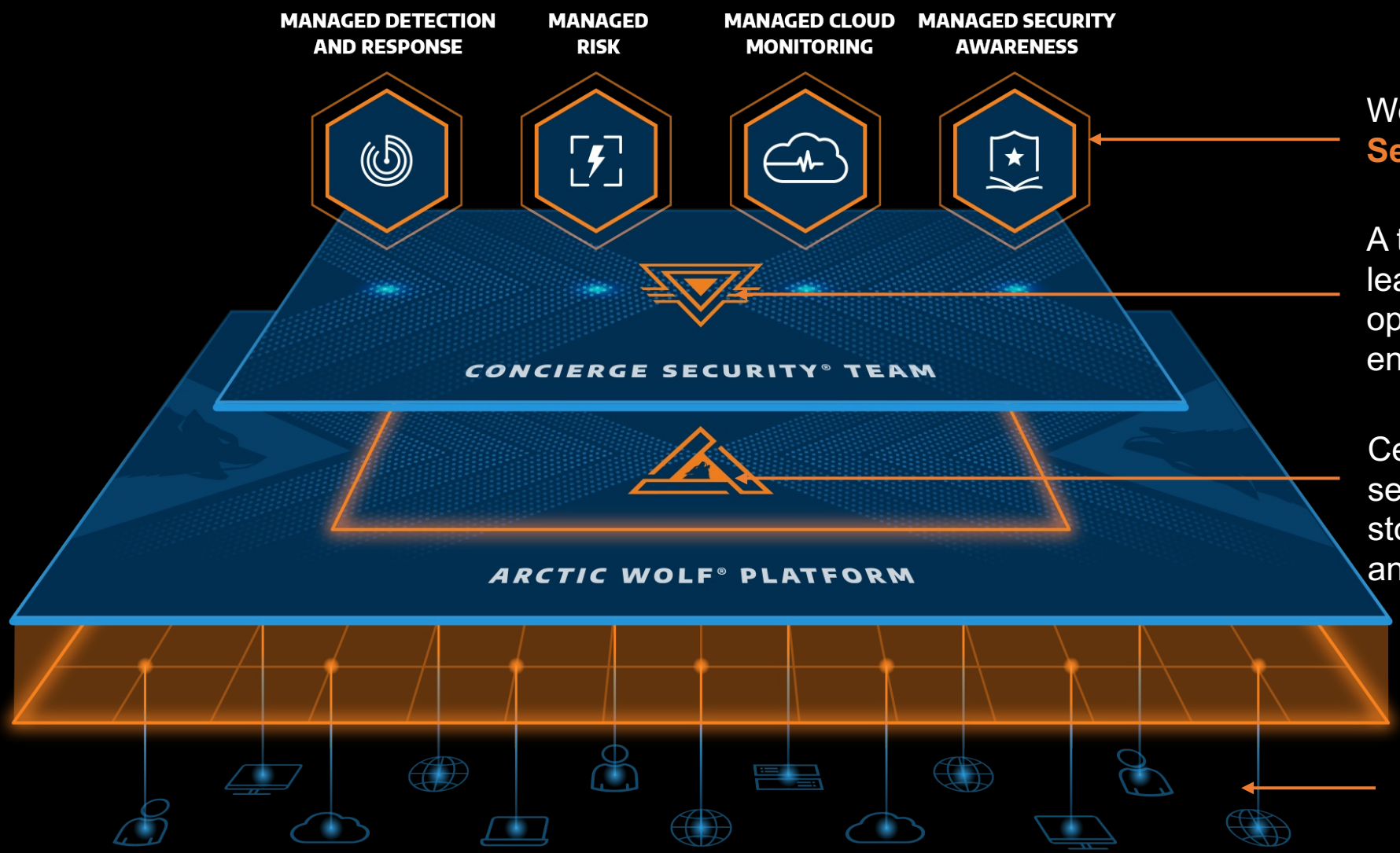
**European SOC**

**Frankfurt, Germany**

- **3,500+ Customers**
  - 260+ of which are in MN
  - Several Lake Conference schools are already customers
- **2000+ Employees**
  - 460+ located at Eden Prairie HQ
  - Local Executive Leadership Team
  - World Class SOC and Executive Briefing Center at HQ
  - Professional Svcs / Onboarding Team



# Arctic Wolf Platform




We deliver services across the entire **Security Operations framework**

A team of assigned security experts who learn your organization and continually optimize your security posture for your environment

Centralize all data in our cloud-native security analytics platform for 24/7 storage, enrichment, correlation, analysis and investigation

Leverage your existing technology stack to gain broad visibility across attack surfaces: endpoint, network, cloud, identity & human

# Security Operations at Scale

**2+**
Trillion events per week

**2.5+**
Petabytes processed/week

**>1.3M**
AW active agents and 12,500 sensors

**10 YRS**
Of development / SOC2 Type and ISO 27000

**60+**
Security stack integrations

**>700K**
Tailored reports created for >3k customers

**83%**
Of tickets come from AW detections

## UNMATCHED POWER

## ARCTIC WOLF® PLATFORM

## UNIQUE PRECISION

**1 Ticket**
Per day on average

**99.9%**
True positives

**Single**
View into your security stack

# Reducing the Impact and Likelihood of Cyber Risk

### DWELL TIME

**0:30**

Industry average time to identify an intrusion is 206 days. Arctic Wolf does it in 30 minutes or less.

### TIME OF ATTACKS

**35%**

Threats that were detected after 8PM and before 8AM by Arctic Wolf

### ADVANCED THREATS

**43%**

Of customers have advanced threat activity being missed by security tools but caught by Arctic Wolf

### ACCOUNT TAKEOVER

**70%**

Of customers have some PII exposure and 5.5% have plaintext passwords exposed online

### UNPATCHED VULNERABILITIES

**35%**

Reduction in time to patch critical vulnerabilities after activating Arctic Wolf

### PHISHING

**18%**

Of customers have phishing activity that is missed by email security but caught by Arctic Wolf

# Arctic Wolf Service Offerings

## Managed Detection and Response

The purpose of this solution is to help you defend against advanced threats that bypass prevention tools. We fundamentally believe that you can't have protection if you don't have detection first.

**Detect**

Leverage your existing tech stack to identify advanced network, endpoint, and cloud threats

**Respond**

24x7 coverage and guided response stops threats before they can do harm

**Recover**

Find root cause, validate remediation, and collaborate to continuously improve your overall security posture

**70%** **of new customer environments have latent threats**

## Managed Cloud Monitoring

This solution extends our MDR and Managed Risk capabilities to the cloud, identifying misconfigurations and other vulnerabilities, and monitoring for attacks and account compromises in progress.

**Identify**

Identify exposed cloud platforms and accounts to understand risks, such as unsecured S3 buckets and unauthorized cloud deployments

**Monitor**

Monitor IaaS services for configuration risks, and SaaS apps for key threats and indicators of compromise

**Simplify**

Streamline cloud security with cloud experts plus concierge deployment and management

**47%** **of the incidents we detect include a cloud component**

## Managed Risk

Managed Risk is designed to help you prevent incidents in the first place. We know this capability is badly needed because the Center for Internet Security says that 80% of breaches could have been prevented if the organization had met the top 5 CIS controls.

**Discover**

Identify and categorize risky software, assets, and accounts

**Benchmark**

Understand your current digital risk posture and identify gaps relative to best practices

**Harden**

Know when you're exposed and prioritize security posture improvements

**80%** **of threats can be prevented by meeting the top 5 CIS controls**

## Managed Security Awareness

End the cyber risk of social engineering attacks and human error by preparing every employee to be an active participant in your security posture and strengthen your cyber resilience.

**Engage**

Educate and prepare employees to stop social engineering attacks, like phishing.

**Measure**

Identify employees that fall behind and determine which threat topics require reinforcement.

**Transform**

Achieve a culture of security and strengthen cyber resilience.

**85%** **of data breaches result from employee actions**

# Security Operations Outcomes that Matter to You

## IDENTIFY

You need an accurate picture of your threat posture and exposures across all attack surfaces

## PROTECT

You need confidence that you have things secured & configured properly

## DETECT

You need the ability to spot threats early; both commodity and APTs

## RESPOND

You need to respond to threats and intrusions quickly and efficiently

## RECOVER

You need experience and capabilities to ensure you can get back to business - fast & implement improvements

## Security Operations Framework

# Different Approaches to ‘Security Operations’

| | Security Operations framework coverage | Tech Stack & Compatibility | Visibility across attack surfaces | Pricing | Service Delivery Engagement |
|---|---|---|---|---|---|
| SIEM |  |  |  |  |  |
| MSSP |  |  |  |  |  |
| EDR |  |  |  |  |  |
| MDR |  |  |  |  |  |
| XDR |  |  |  |  |  |
| Arctic Wolf |  |  |  |  |  |
|  | Coverage across Sec Ops framework | Use existing tech and or AW tech | Endpoint, network, Cloud, Apps, Identity and People | Unlimited & unmetered data pricing | Invented Concierge Security Team |





# Why Arctic Wolf MDR is a better value



| Capability | Arctic Wolf MDR | Others |
|---|---|---|
| Network Traffic Analysis (NTA) | Included with our sensor | NIDS/HIDS only (NTA is add-on) |
| Asset Inventory across endpoint & network | Included | Typically “either/or” |
| Vulnerability Scanning | Included | May not include active monitoring & detecting vulnerability as part of core |
| Holistic Visibility includes network, endpoint, cloud, log sources, behavioral sources | Included | May incur additional costs |
| Integrations | Unlimited (true vendor neutrality) | May require specific app integrations |
| Engagement with CST | Unlimited, direct access | No CST (trained analysts are not equivalent); call center 800 # vs. direct access |
| Remote Incident Response | Unlimited | Typically capped |
| Security Guidance, Support, Analysis | Unlimited | Typically capped |
| Custom rules allowed | Unlimited | May be capped |
| Log ingestion & Log data volume | Unlimited | Typically capped |
| Log bandwidth | Unlimited | May be capped |
| Security Posture Reviews | Unlimited* | Typically capped |
| Dark web scanning & account takeover monitoring | Included | Typically requires 3rd party |



* Default is once per month, but customers can request more frequent reviews



# Why Arctic Wolf?

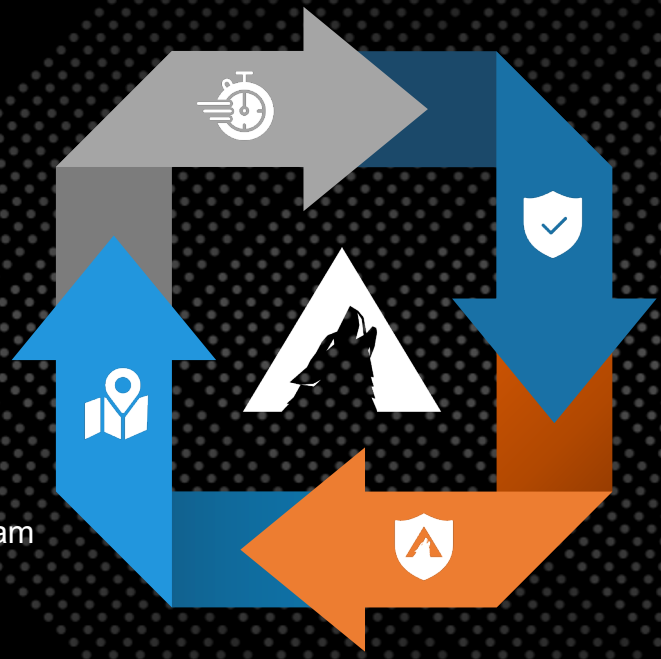
Our innovative Security Operations platform and concierge delivery model enable you to end Cyber Risk

## Time to Value

- Leverage existing investments
- Add resources & expertise to your team
- Reduce noise & drive efficiency

## Guidance

- Concierge Security Team
- Framework tailored to your environment
- World-class expertise on-demand

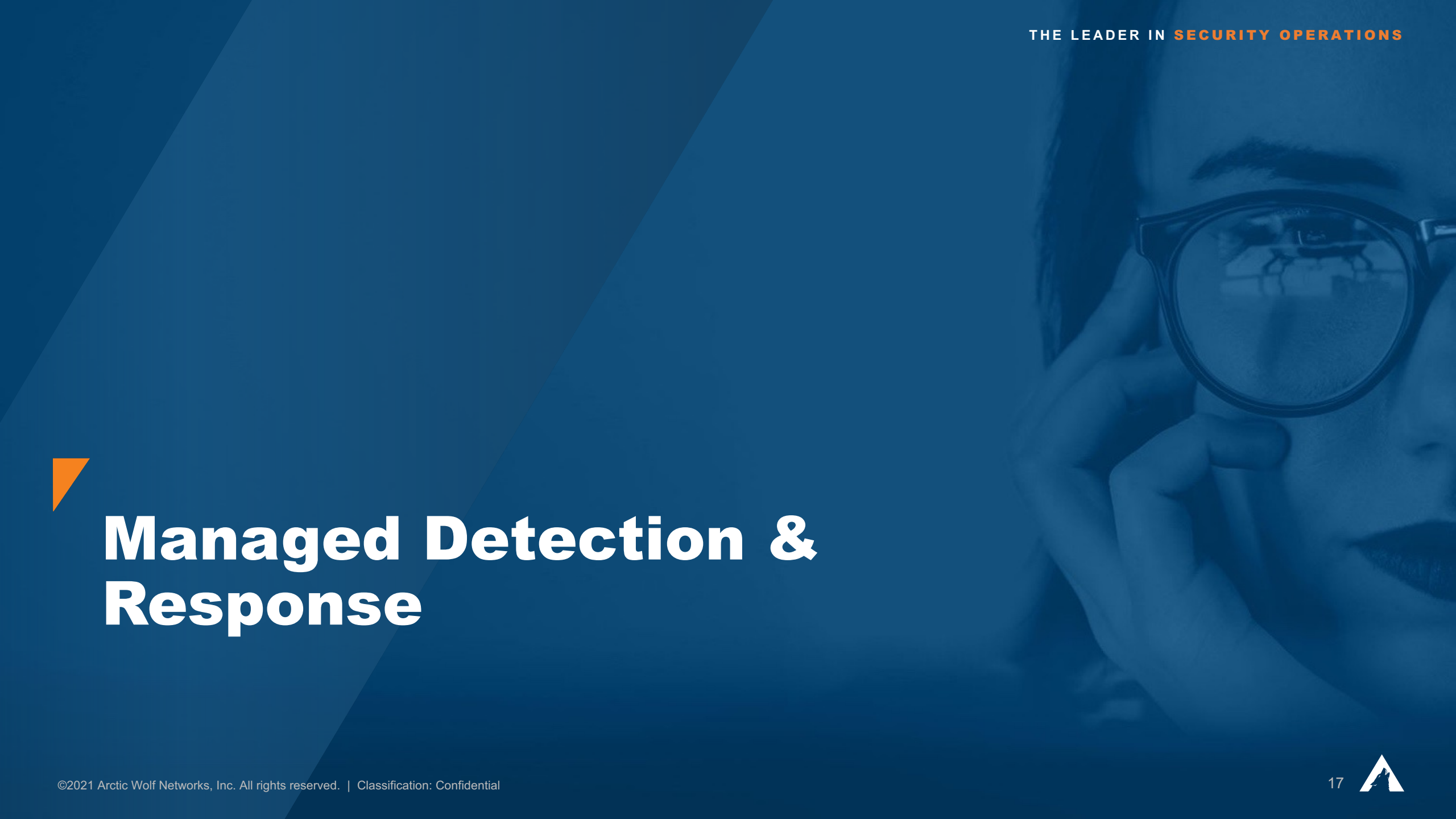


## Protection

- Against commodity & advanced threats
- Attack surfaces
- All-the-time (24x7)

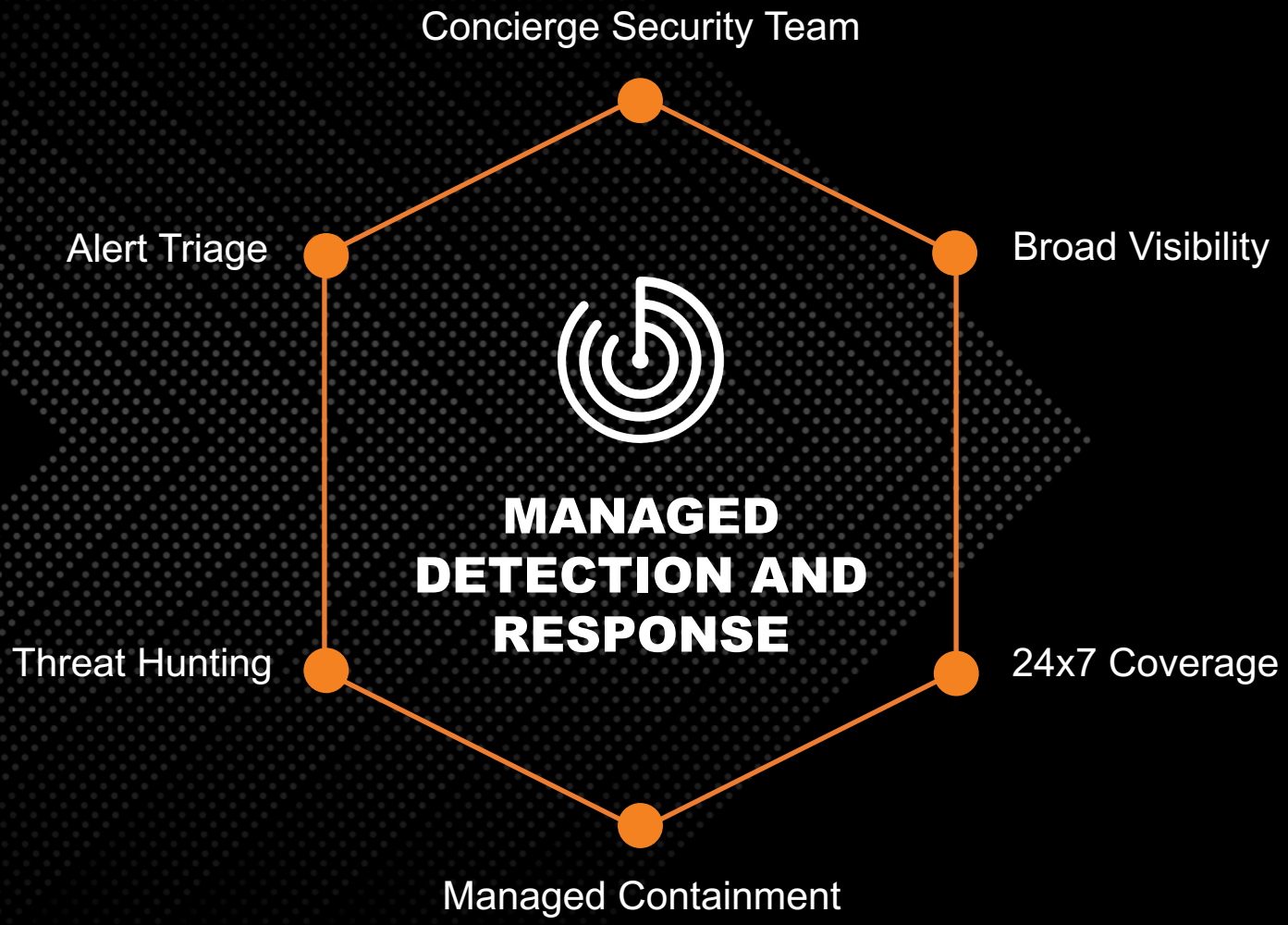
## Resilience

- Proactive risk mgt
- Continuous posture assessment
- Sustained compliance



# Managed Detection & Response

# Arctic Wolf Solutions




## Detect

Leverage your existing tech stack to identify advanced network, endpoint, and cloud threats

## Respond

24x7 coverage and guided response stops threats before they can do harm

## Recover

Find root cause, validate remediation, and collaborate to continuously improve your overall security posture

**70%**

of new customer environments have latent threats

# MDR Architecture

Edina Public Schools
DEFINING EXCELLENCE

Triage Team

Arctic Wolf Platform
90 Day Log Retention

Concierge Security Team (CST)

3 Physical Sensors

On-Premise Logs

Cloud

SaaS Integrations

Flow Data

IDS Packet Analysis

HTTP, DHCP, FTP

Host Identification (NMAP)

Device Inventory

FORTINET

AD DNS Logs

Active Directory

CARBON BLACK

Azure

Azure Security Center

Azure Active Directory

Log Search

Access point

Syslog

Office 365

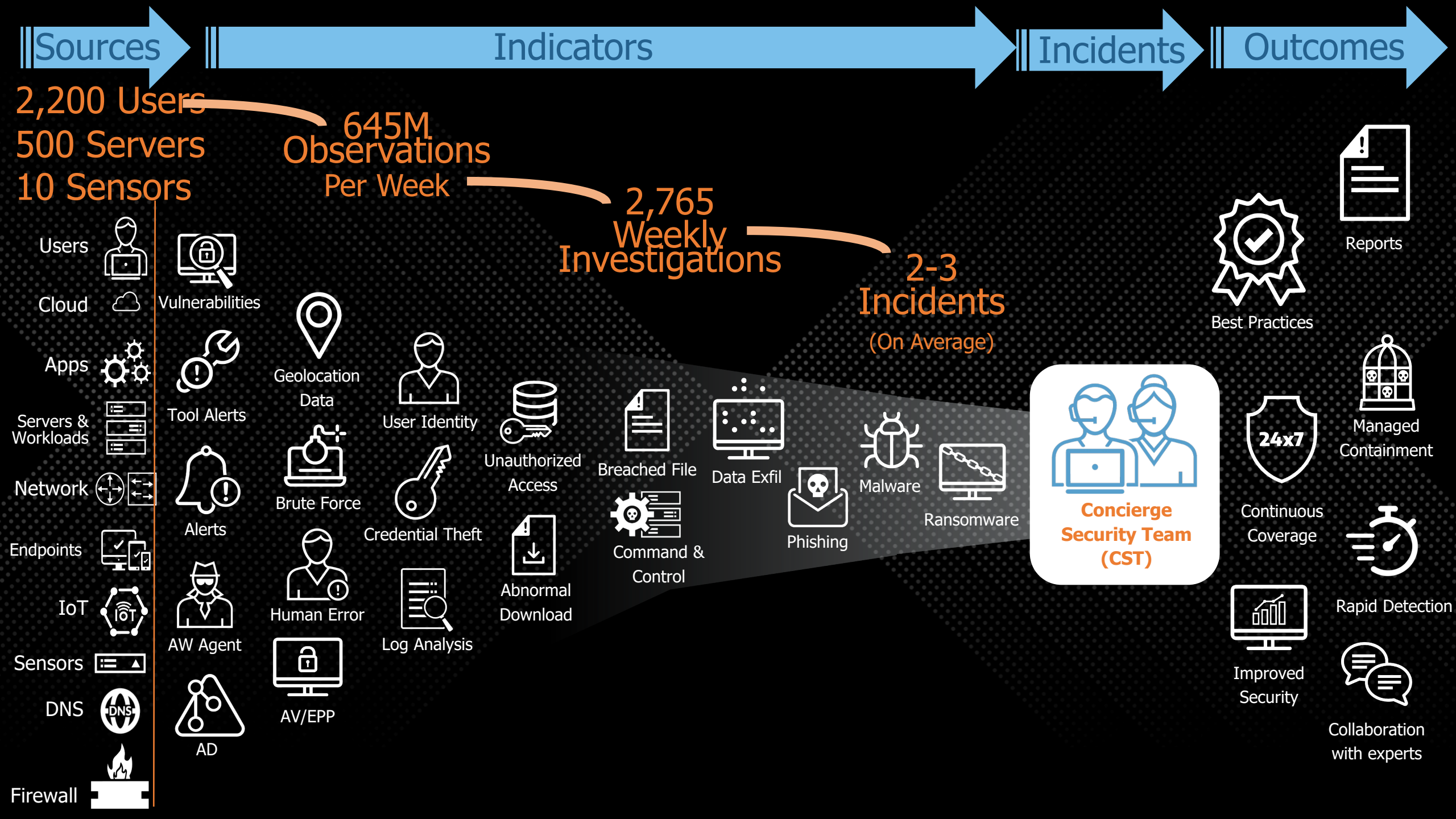
Azure MFA

External Scanning

Vulnerability Data

Dark Web Data

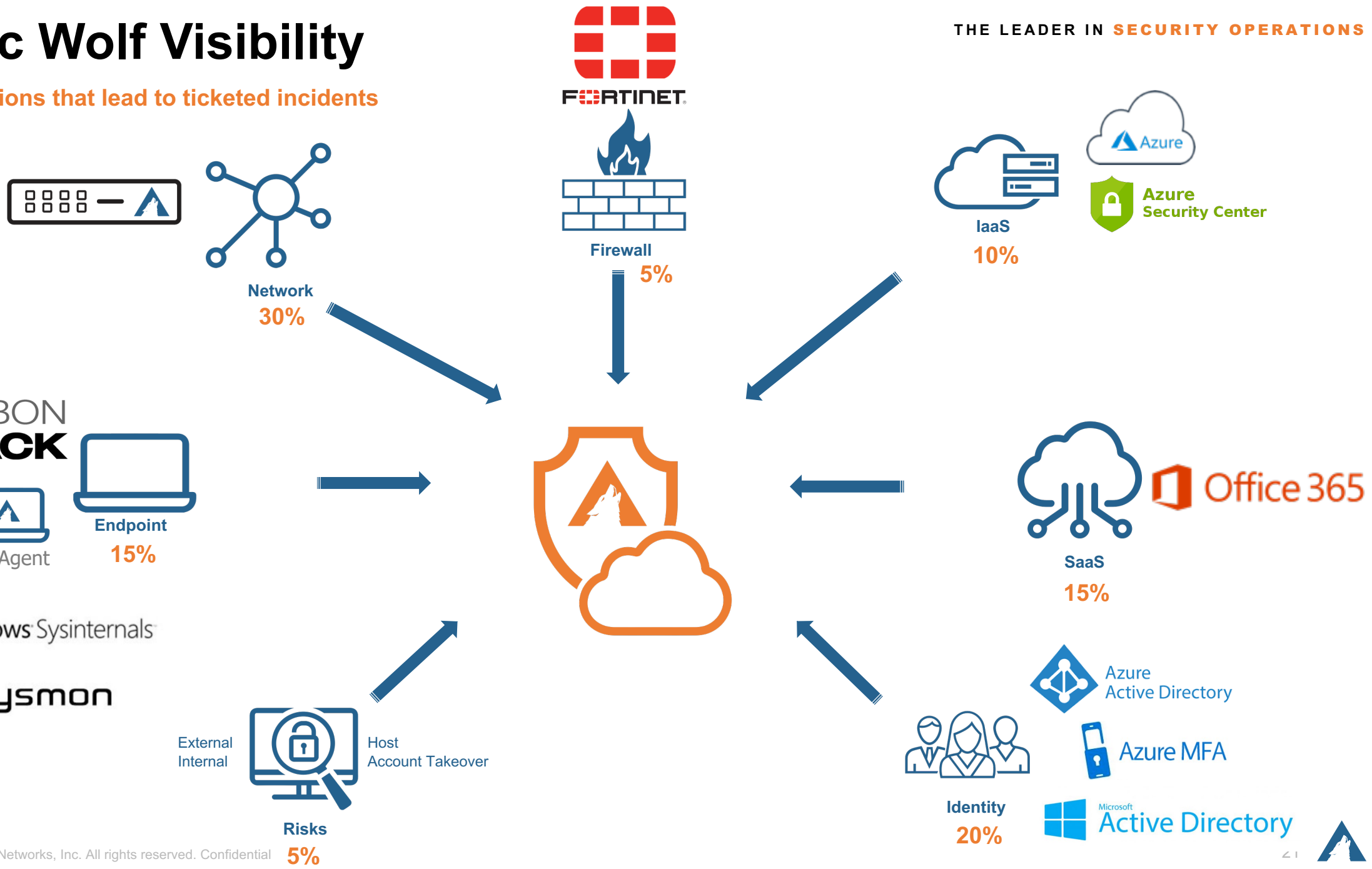
Publicly Accessible Ports/Services


Sources
Indicators
Incidents
Outcomes
2,200 Users
500 Servers
10 Sensors
645M
Observations
Per Week
2,765
Weekly
Investigations
2-3
Incidents
(On Average)
Users
Cloud
Apps
Servers &
Workloads
Network
Endpoints
IoT
Sensors
DNS
Firewall
Vulnerabilities
Tool Alerts
Alerts
AW Agent
AD
Geolocation
Data
Brute Force
Human Error
AV/EPP
User Identity
Credential Theft
Log Analysis
Unauthorized
Access
Abnormal
Download
Breached File
Command &
Control
Data Exfil
Phishing
Malware
Ransomware
Concierge
Security Team
(CST)
Best Practices
Reports
24x7
Managed
Containment
Continuous
Coverage
Rapid Detection
Improved
Security
Collaboration
with experts

# Arctic Wolf Visibility



## Observations that lead to ticketed incidents



# Arctic Wolf® Managed Detection and Response

## Includes:

- Fully managed and hosted SIEM
- 24x7x365 monitoring
- Named Concierge Security Team to augment your team
- 550+ SOC experts monitoring your data
- Integrations into over 160+ security tools
- Monthly External vulnerability scanning
- Continuous Dark Web scanning for harvested credentials
- Monthly and quarterly reporting
- Ad hoc reports generated at your request
- Monthly Security Posture in Depth Reviews
- Unlimited log volume and events per second
- 90-day standard log retention
- Unlimited number of custom rules
- Managed IDS
- Containment capabilities


DATASHEET

Arctic Wolf Managed Detection and Response Solution

Threat Detection and Response Delivered by the Concierge Security Team

The Arctic Wolf Concierge Security Team has found latent threats lingering in 73% of our customers' environments within the first 90 days of the engagement.

Concierge Security Team

Leverage Existing Infrastructure

Advanced Threat Detection

Managed Containment

Detect

Respond

Recover

# The AW Concierge Model

# The Concierge Model


## BENEFITS

**Dedicated security operations resource**

**Tuning & optimization**

**Deliver threat intelligence and situational awareness**

**Implement a proactive Security Journey**

# Security is a Journey; not a destination


- Cyber Risk Reduction
- Ensuring Insurability
- Fast Time Security Value
- Eliminate Blind-spots

# Concierge Security Team (CST)


Your named Concierge Security Team will work with you to build and execute a Security Journey that meets your organization's goals and objectives while identifying opportunities to strengthen your security posture over time.

## EXPERTISE

Deliver execution and operational excellence with skills required to detect advanced threats and manage risks in a way that's customized to your environment.

### Security Operations Experts

Hundreds of years of combined experience with cybersecurity accreditations like CISSP, HCISPP, CCSP, CISM, CRISC, GCIH

### Threat Hunting

Hunting for suspicious activity across your environment

### Informed Incident Insights

Filter out the noise to reveal what happened, and what to do about it

## STRATEGY

Strategic security guidance drives continuous improvement that's tailored to the specific needs of your organization.

### Security Posture Reviews

Evaluate the root cause of threats and get prioritized recommendations to improve posture

### Named Advisors

Trusted security operations experts paired with you to deliver tailored triage and strategic guidance

### Security Journey Guidance

Quarterly reviews to help you design, implement, and achieve your security vision

# Arctic Wolf Triage Team


The Triage Team works 24x7x365 to investigate alerts generated by the Arctic Wolf Platform. This team provides tactical support and guidance to customers and the Concierge Security Team during security events.

## COVERAGE

Work around the clock to triage critical events and deliver actionable insights when you need them the most.

### 24x7 Continuous Monitoring

Your environment is monitored around the clock for threats and risks

### Rapid Response

Investigate and escalate critical events within thirty minutes

### Real-Time Remediation

Rapidly contain incidents and get detailed guidance on remediation

### On- Demand Access

To security analysts via telephone or email 24/7

## INVESTIGATION

Deliver execution and operational excellence with skills required to detect advanced threats and manage risks in a way that's customized to your environment.

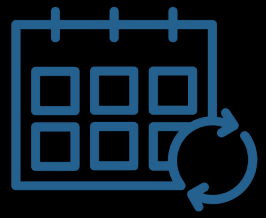
### Security Operations Experts

Top-talent with hundreds of years of combined experience working for Military, Government and Public and Private sector organizations.

### Informed Incident Insights

- Filter out the noise to reveal what happened, and what to do about it
- Detect threats across network, endpoint, & cloud.
- Expert analysis of IOCs across entire attack surface using a purpose-built cloud platform
- Discover vulnerabilities and misconfigurations

# What will the Concierge Team do for you?



Regular Meetings

Strategic security and support interactions

Periodic analysis conducted against your data

Inside knowledge about current cyber landscape and trends

Help improve your Vulnerability and Risk Management Programs

# S2 = cSOC & Concierge

## Whom does what?

### cSOC Triage Team

- Handles Security Incidents and Investigations 24x7
- Works with ALL customers
- Outlines actionable remediation for customers / CSTs
- Reports, whitelisting, ad-hoc requests, onboarding, sensor validation
- Focuses on customer SLAs
- Linearity staffing 24x7

- Actively working with customers
- Engage CST during security incident

### Concierge Security Team ('CST')

- Customer specialists
- Extension of internal team
- Focused value-added services
- Deep Dives / Meaningful Conversations, Customizations

- Strategic consulting with customers
- Security journey of customers

# About our S2 team

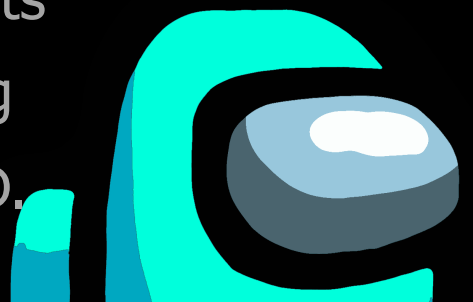
## Why does your S2 'Love' Arctic Wolf

- Low turnover in the cSOC & Concierge
- We limit customer load to ensure each S2 can respond to customer support needs.
- You are assigned a S2 team directly after onboarding
- Common Certifications held by the team
  - CompTIA Security+
  - GIAC Certified Incident Handler
  - EC-Council Certified Ethical Hacker
  - GIAC Network Forensics Analysis
  - CCNAS
  - CISSP



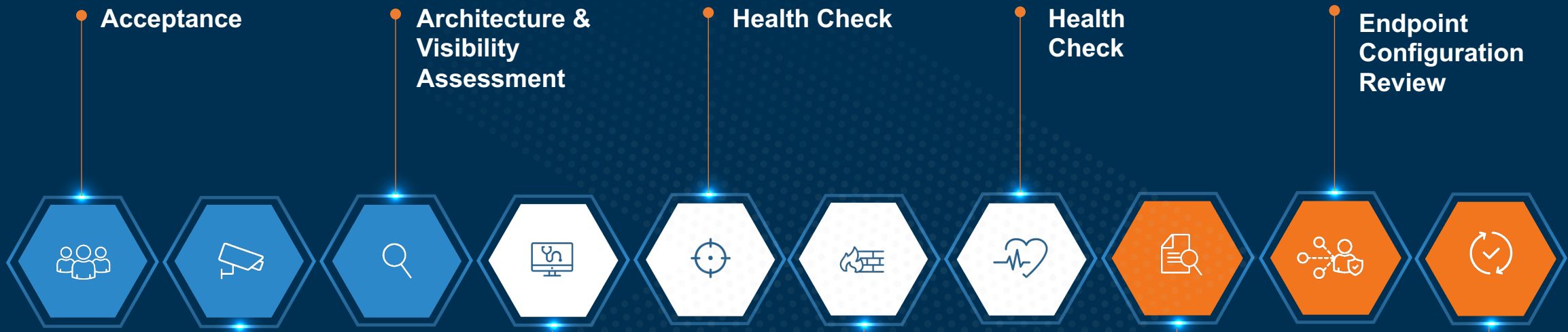
## Why we love our JOB:

- S2 Game Night
- S2 Culture
- S2 Culture COINS
- Hackathon
- Lego Kits
- Training
- Alpha D.

# Customization Focus

Core
Fundamentals
Optimized



- Acceptance
- Concierge Kickoff
- Architecture & Visibility Assessment
- Log Source Review
- Health Check
- Firewall Configuration Review
- Health Check
- Active Directory Configuration Review
- Endpoint Configuration Review
- Security Journey Validation

# Steady State Focus

- Business Email Compromise
- Active Directory Password Policy Audit W/ Identity & Lifecycle Mgmt.
- O365 Security Recommendations
- Backup Best Practices & Recommendations
- Health Check
- Ransomware and Malware Hardening
- Cloud Data Loss Prevention
- External Assessment
- O365 Mail Forwarding Rules Audit
- CIS Benchmarks